Norman Virus Control for Workstations

Version 5.8

User's Guide

Limited warranty

Norman guarantees that the enclosed diskette/CD-ROM and documentation do not have production flaws. If you report a flaw within 30 days of purchase, Norman will replace the defective diskette/CD-ROM and/or documentation at no charge. Proof of purchase must be enclosed with any claim.

This warranty is limited to replacement of the product. Norman is not liable for any other form of loss or damage arising from use of the software or documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

With regard to defects or flaws in the diskette/CD-ROM or documentation, or this licensing agreement, this warranty supersedes any other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

In particular, and without the limitations imposed by the licensing agreement with regard to any special use or purpose, Norman will in no event be liable for loss of profits or other commercial damage including but not limited to incidental or consequential damages.

This warranty expires 30 days after purchase.

The information in this document as well as the functionality of the software is subject to change without notice. The software may be used in accordance with the terms of the license agreement. The purchaser may make one copy of the software for backup purposes. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman.

The Norman logo is a registered trademark of Norman ASA.

Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

NVC documentation and software are

Copyright © 1990-2005 Norman ASA.

All rights reserved.

Last revised on 23 February 2005.

Norman Offices

Norman Data Defense Systems AS
Blangstedgårdsvej 1, DK-Odense SØ, **Denmark**
Tel. +45 6311 0508 Fax: +45 6590 5102
E-mail: normandk@normandk.com Web: http://www.norman.com/dk

Norman Ibas OY
Läkkisepäntie 11, 00620 Helsinki, **Finland**.
Tel: +358 9 2727 210 Fax: +358 92727 2121
E-mail: norman@norman-ibas.fi Web: http://www.norman.fi

Norman Data Defense Systems GmbH
Kieler Str. 15, D-42697 Solingen, **Germany**.
Tel: +49 212 267 180 Fax: +49 212 267 1815
E-mail: norman@norman.de Web: http://www.norman.de

Norman/SHARK BV
Postbus 159, 2130 AD, Hoofddorp, **The Netherlands**.
Tel: +31 23 789 02 22 Fax: +31 23 561 3165
E-mail: support@norman.nl Web: http://www.norman.nl

Norman ASA
Mailing address: P.O. Box 43, N-1324, Lysaker, **Norway**.
Physical address: Strandveien 37, Lysaker, N-1324 Norway.
Tel: +47 67 10 97 00 Fax: +47 67 58 99 40
E-mail: norman@norman.no Web: http://www.norman.no

Norman Data Defense Systems AB
P.O. Box 5044, SE-194 05 Upplands Väsby, **Sweden**
Tel. +46 11 230 330 Fax: +46 8 87 52 52
E-mail: support.se@norman.no Web: http://www.norman.com/se

Norman Data Defense Systems AG
Postfach CH-4015, Basel, **Switzerland**.
Tel: +41 61 487 2500 Fax: +41 61 487 2501
E-mail: norman@norman.ch Web: http://www.norman.ch

Norman Data Defense Systems (UK) Ltd
PO Box 5517, Milton Keynes MK5 6XJ, **United Kingdom**.
Tel: +44 08707 448044 Fax: +44 08717 176999
E-mail: norman@normanuk.com Web: http://www.normanuk.com

Norman Data Defense Systems Inc.
9302 Lee Highway, Suite 950A, Fairfax, VA 22031, **USA**
Tel: +1 703 267 6109, Fax: +1 703 934 6367
E-mail: norman@norman.com Web: http://www.norman.com/us

Training and Technical Support

For training or technical support, please contact your local dealer or Norman ASA.

Copyright © 1990-2005 Norman

Conventions

Paragraphs that are clearly intended for users in a network or for the system administrator, and hence of little or no interest for single-users, are identified by a network icon in the left margin.

This manual is intended for Windows' as well as OS/2 users. Whenever platform specific differences affect NVC, this icon in the margin denotes a special consideration for OS/2.

System requirements

This version supports installation of NVC v5 on Windows 95/98/Me, Windows NT/2000/XP/2003 machines, Linux, OS/2 Warp 4, OS/2 Warp Server, Workspace On-demand, and eComStation.

For Windows 95 WinSock2 must be installed, Internet Explorer 5.5 is recommended.

For Windows NT, version 4 with SP4 (or higher) and Internet Explorer 4.0 (or higher) are required.

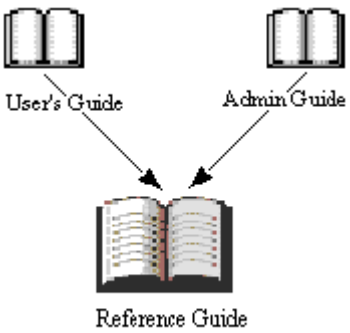
For OS/2 we recommend Warp 4 fp 15 (or higher) and Java 1.1.8.

For Linux, glibc 2.2 is required.

In general, we recommend that you use the newest Service Pack / security-related updates for your platform.

Copyright © 1990-2005 Norman

Who should read this manual?



This manual is primarily aimed at end-users who want a brief introduction to NVC's basic functionality without getting too technical. All main functions are outlined, including the installation procedure.

Other NVC manuals

In addition to this manual, the *Administrator's Guide* covers topics that are particularly useful for those responsible for network installations. Finally, the *Reference Guide* provides detailed information on all functions found in NVC, and this manual is useful for administrators as well as single-users.

Prerequisites

To take full advantage of all the functions in NVC, you should have some experience with your operating system and applications that run on this platform.

NVC is designed to work with the operating system at all levels, and you will find that basic Windows or OS/2 functionality is reflected in the program.

What is NVC?

Norman Virus Control (NVC) is an anti-virus program that monitors your PC for malicious software, also referred to as ***malware***. For the sake of simplicity, we often use the term ***virus*** as a collective description of unwanted code. The most common types of malware are viruses, worms, and trojans. NVC can detect and remove known and unknown viruses from hard disks, floppy disks, e-mail attachments, etc.

NVC checks files when they are accessed, and possible viruses are removed automatically. If NVC is unable to clean an infected file, you will receive a warning and instructions on how to proceed.

You can—and we encourage you to do so—perform manual scans of selected areas of your machine, and use the task editor and scheduler to define what to scan and when.

Copyright © 1990-2005 Norman

Note: NVC is shipped with pre-selected settings that we consider sufficient to protect you against virus attacks. Most settings are configurable, so that you can set up NVC to suit your needs.

Technical support

Norman provides technical support and consultancy services for NVC and security issues in general. Technical support also comprises quality assurance of your anti-virus installation, including assistance in tailoring NVC to match your exact needs.

Note that the number of services available will vary between the different countries.

Copyright © 1990-2005 Norman

Contents

Conventions iv
System requirements iv
Who should read this manual? v
What is NVC? v
Technical support vi

NVC programs and modules 9

NVC overview 10
Shortcut to NVC modules and scanning 10

Installing NVC 13

Components 13

The configuration editor 15

Install and update product 16

Norman Program Manager 17

Components 17
Messages 18
E-mail, SMS, SNMP 18

Norman Virus Control 19

Components 19
Common settings 19
The On-demand scanner 20
The On-access scanner 21
Norman Internet Protection 22

Copyright © 1990-2005 Norman

Enable NIP 23

Norman Quarantine 25

Quarantine 25

The task editor 26

About the scheduler 27

Utilities 28

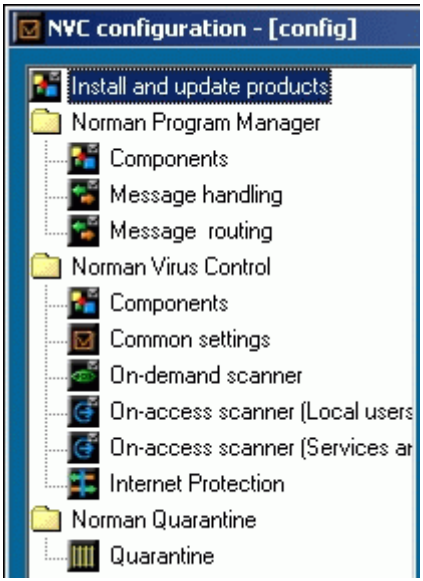
Internet Update 29

Other functions 30

NPM - the agent 30
The Command line scanner.... 31
What is a sandbox? 31

Copyright © 1990-2005 Norman

NVC programs and modules



This chapter presents how NVC—and possible other Norman products—are presented in the configuration editor and under the Norman icon in the system tray. On the left hand side of the editor a list of products and modules/components appears. The list will display which Norman products you have installed, and the corresponding components and modules for each program are organized as *folders*—with the same logic and appearance as in a Windows Explorer environment. The modules are made up of one or more tabbed dialogs where the configuration options are located.:

When you select one of the entries on the left hand side, the configuration options for the selected module appears on the right hand side of the dialog.

Norman Program Manager incorporates modules that can be shared by different Norman programs or plug-ins ready to be included in this user interface. The modules in this folder are controlled by ***Zanda*** (Zero Administration Network Distribution Agent).

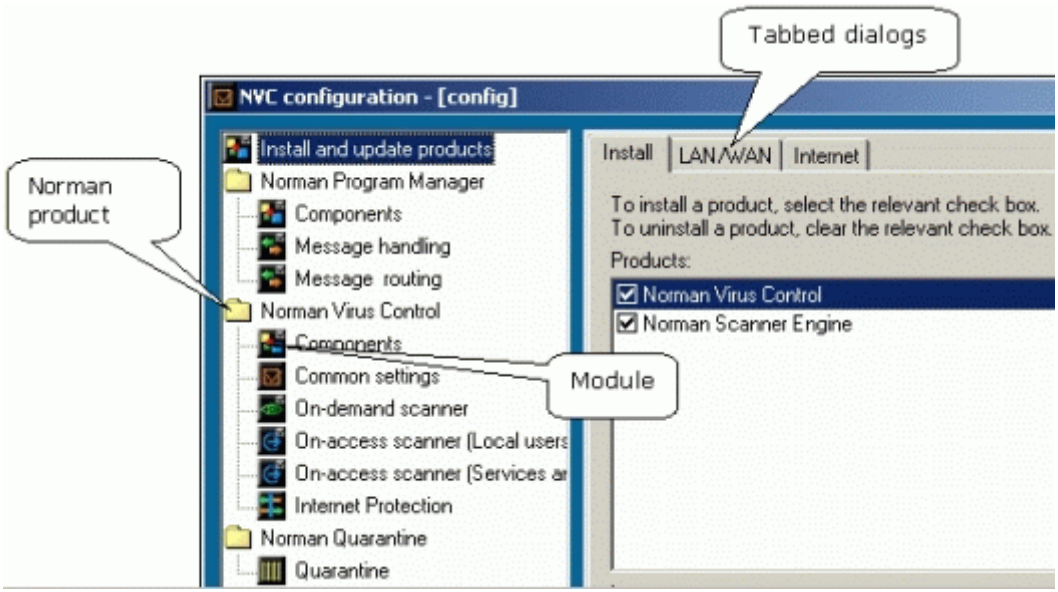
⇨ 'NPM - the agent' on page 30.

The product-specific modules are listed under **Norman Virus Control**. Please refer to page 19.

Copyright © 1990-2005 Norman

NVC overview

As explained in the previous section, the user interface for NVC v5.8 appears like this:



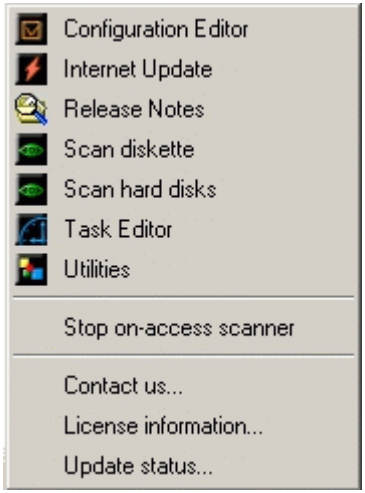
Shortcut to NVC modules and scanning

During setup, a Norman icon is placed in the system tray in the lower right-hand corner of the screen. This icon confirms that NVC is installed on this machine. See also page 11.

OS/2: NVC appears as an entry in the desktop menu. Right-click on the desktop and select *Norman Virus Control*.

The items listed above the separation line on the menu that appears when you click on this icon, are copies of the items that at any time appear on the Start|Programs|Norman Virus Control menu.

Copyright © 1990-2005 Norman



This is a shortcut to NVC's main modules, as well as some typical NVC tasks. In Windows, right-click the mouse button to display this menu. It gives easy access to NVC modules and scanning tasks. You can **Start/stop the on-access scanner** by a simple mouse click. Select **Contact us** to display contact information about our offices and distributors on Norman's web site, or view the license. Finally, you can view update status for the Norman product(s), including key information for the virus definition files.

Warnings

The Norman icon also provides information regarding the state of your NVC installation. If the icon appears like this:

it denotes that the NVC components currently running do not match those selected in the **Start** tab in the Configuration editor's **Norman Virus Control|Components|Start**. If the Norman 'N' appears with the red symbol blinking, place the pointing device on the symbol, and NVC informs you which component that needs updating or possible other error situations.

Note: During startup, the red symbol is visible until all modules have started. The older and slower the machine, the longer it takes for all modules to load. However, the "normal" symbol should appear after a maximum of 1-2 minutes.

For Windows XP users who have installed SP2: Microsoft included its "Security Center" with options and features for

Copyright © 1990-2005 Norman

Firewall, automatic updates and virus protection. NVC is one of the AV vendors that the operating system detects. If NVC's virus definition files are outdated or the on-access scanner is not running, you will also receive a warning from Windows that something is wrong. The Security Center symbol appears, and you can click on it to view and edit the Windows settings.

If this icon appears in the system tray,

it signifies that one of these situations have occurred:

1. The On-access scanner is installed, but has been manually disabled. To start the On-access scanner, select the shortcut from the menu, or go to the Start tab in the Configuration editor's **Norman Virus Control|Components|Start**. Select *On-access scanner* and click **Save**.
2. You have probably selected **Reboot later** on a previous prompt, and NVC is waiting for a reboot.
3. An installation error that a reboot might fix.

Outdated virus definition files

A *blinking* yellow triangle signifies that the virus definition files are outdated, i.e. they are at least ten days old. The same happens if the On-access scanner is turned off.

Informational icons

When the Norman icon appears with a cog, Norman Program Manager is working with the program, most likely an update. We do not recommend that you turn off your machine when NPM is working, i.e. while this symbol is visible.

Please refer to the *Reference Guide* for a complete overview of possible symbols that might appear in the system tray.

Copyright © 1990-2005 Norman

Installing NVC

The setup program uninstalls possible older NVC versions found during installation.

The following chapter will guide you in installing Norman Virus Control (NVC).

1. Insert the CD-ROM into its drive.

Note: If you download the program from the web, double-click the downloaded file and proceed to step 4.

2. Autorun launches the installation program.
3. If you have disabled Autorun, click on Start|Run, enter the CD-ROM drive letter (for example **d:**) and type `norman.exe`. Click **OK**
4. Follow the directions on the screen.

During the installation procedure, you will be prompted to enter an authentication key. The key defines which products and modules you are licensed to. For the typical single-user installing at a stand-alone machine at home, components like **E-mail, SMS, SNMP** and **On-access scanner (Services and remote users)** are not included, and will therefore not appear at all.

When the machine is restarted, the green Norman icon appears in the system tray (down in the right-hand corner).

Components

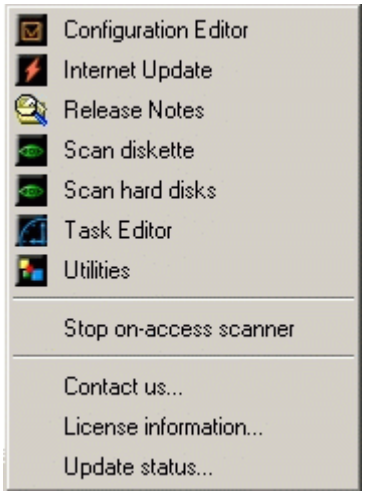
Norman Virus Control (NVC) comes with a set of components that will be installed during setup. When setup is complete, you can remove possible undesired components. NVC is a plug-in based application, and new plug-ins, i.e. programs, are likely to be introduced as new technology and security threats commence.

Common for all tabs:

In a network environment, the **Access field** at the bottom of each tab will appear if you have administrator's rights. The system administrator decides what should be visible and/or configurable

Copyright © 1990-2005 Norman

from the workstations. The average user may therefore view all or some of the tabs, but is not necessarily entitled to change the settings.



You can configure the different functions in NVC from one central point — the Configuration editor. Select *Configuration Editor* from the Norman group/folder that appears when you right-click the green 'N' in the system tray:

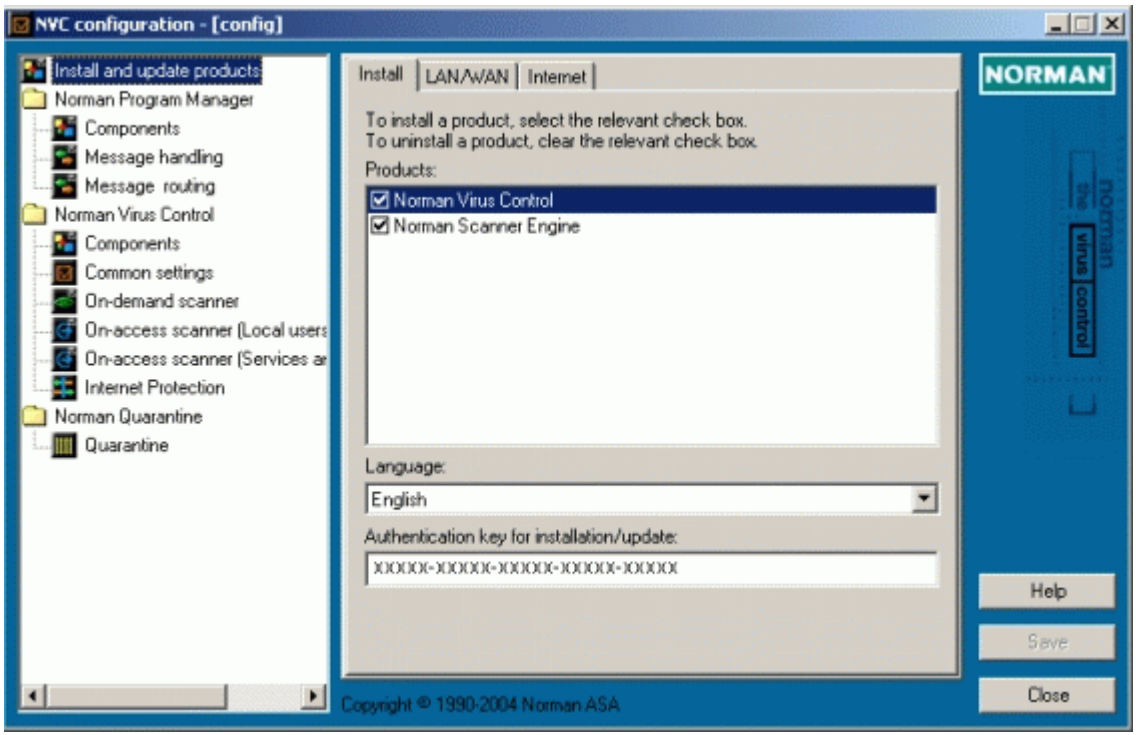
The list inside the dialog box reflects which components you have installed. Components like *Message router* and *E-mail, SMS, SNMP*, for example, will not appear on a single-user, stand-alone installation.

Each component has its own tabbed dialog box with a set of configuration options. Click on the component you wish to configure and make your selections from the corresponding tabbed dialog box.

Copyright © 1990-2005 Norman

The configuration editor

The configuration editor is the core of the program, with install and configuration options, as well as Norman Program Manager (NPM) and messaging options. You can configure all the different functions in NVC from this central point. Like all other NVC groups, right-click on the Norman icon in the system tray and select **Configuration editor** from them menu. Alternatively, select *Start|Programs|Norman Virus Control|Configuration editor*:



Copyright © 1990-2005 Norman

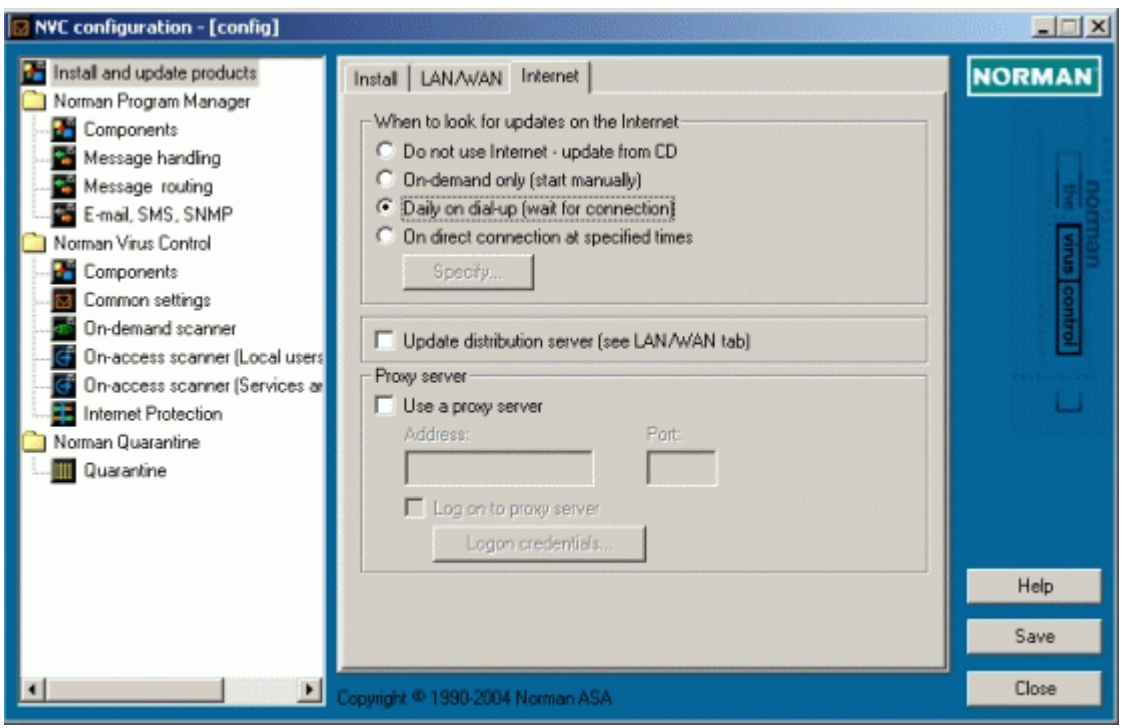
Install and update product

The Installation settings module is made up from three tabbed dialogs:

Install, where you can view, install, or remove available Norman products,

LAN/WAN, for networks, where the system administrator enter details about update frequency, network type, distribution server etc. in order to ensure a safe update of software, configuration, and task file for all machines in the network,

Internet, where you can instruct NVC to update your installation continuously over the Internet. This is where you decide how, when and how often you want to update NVC:



Please refer to the *Reference Guide* for details on this dialog.

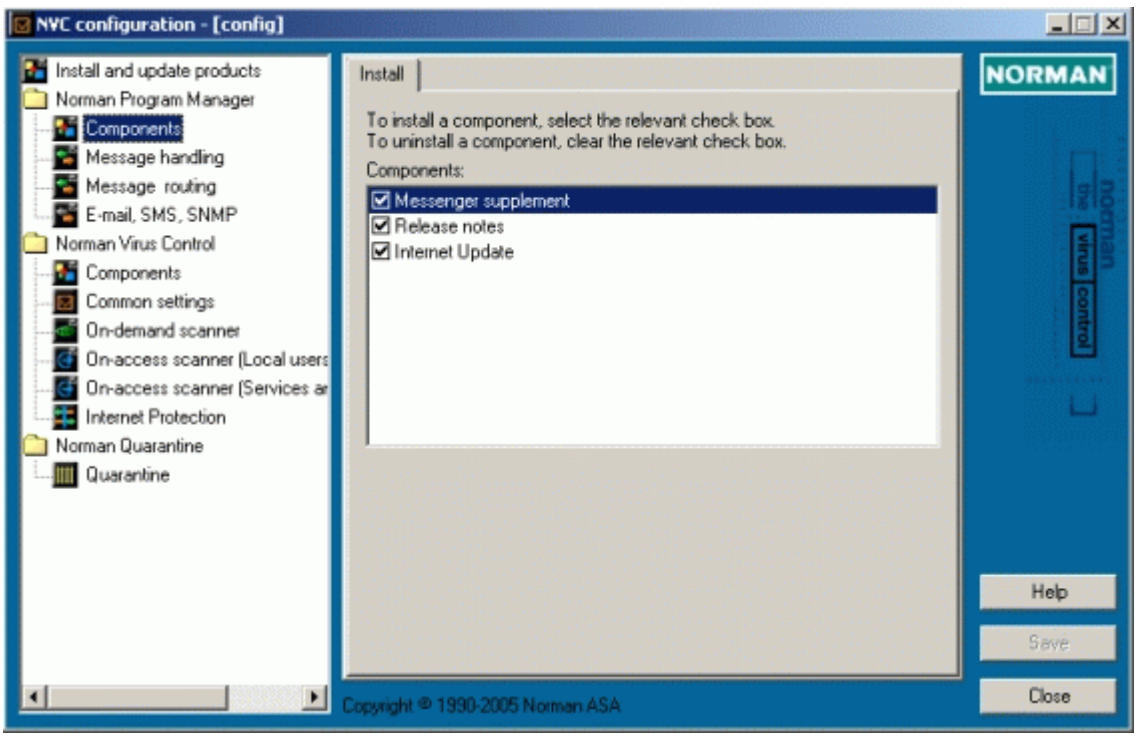
Copyright © 1990-2005 Norman

Norman Program Manager

Components

The Norman Program Manager (NPM) folder is made up from three Norman proprietary modules that handles the internal communication between the different parts of the product.

Even though a module like Message routing is irrelevant to the single home user, the NPM folder as such is vital to NVC's inner working. From **Components** you can install/uninstall NPM-related components.



NPM contains most of the "hidden"—but vital—functions that make NVC work. The single-most important task that the user must do here is making sure that **Internet update** is selected for

Copyright © 1990-2005 Norman

installation. Remember that an outdated anti-virus product is of little or no use at all.

Messages

Message handling is the input module for generating a log file, displaying messages on the message console, and sending a user-defined message when the On-access scanner detects an infection. The first two tabs have identical options. Each of these tabbed dialogs has two sections, one for ***local*** incidents and one for incidents reported from ***other computers***. The selections you make decide what type of incidents are kept in the log file or are displayed on the message console.

E-mail, SMS, SNMP

This module provides the option of sending e-mails or SMS messages about selected events on standalone PCs as well as networked machines. For networks with SNMP, NVC can be configured to send SNMP traps. As for the other messaging modules, you must distinguish between **locally** generated messages and messages **received** from other machines.

Copyright © 1990-2005 Norman

Norman Virus Control

The ***Norman Virus Control*** folder holds many of the modules that you use regularly. The current available modules include:

Components

Select which components you want to install from the list. By default, all components are pre-selected. Remove the check mark for components that you do not want to install. In general, we recommend that you install all available components.

Common settings

The settings in this module affect the behavior of the On-demand and On-access scanner. In this version, the only common component is the **Exclude list**. The Exclude list allows you to enter file names, directories, or entire drives that you wish to exclude from scanning,

Copyright © 1990-2005 Norman

The On-demand scanner

The purpose of the On-demand scanner is to make periodic inspections of selected areas on your system. You can launch the On-demand scanner in different ways:

1. Place the cursor on any file system object, for example in Windows Explorer, click the right mouse button and select *Norman Virus Control* from the menu.
2. Select the Task Editor from the Norman menu and schedule the on-demand scanner to run at a specific time or set intervals.

⇨ ‘The task editor’ on page 26.

3. Use the shortcuts from the Norman menu; **Scan diskette** or **Scan hard disks**.

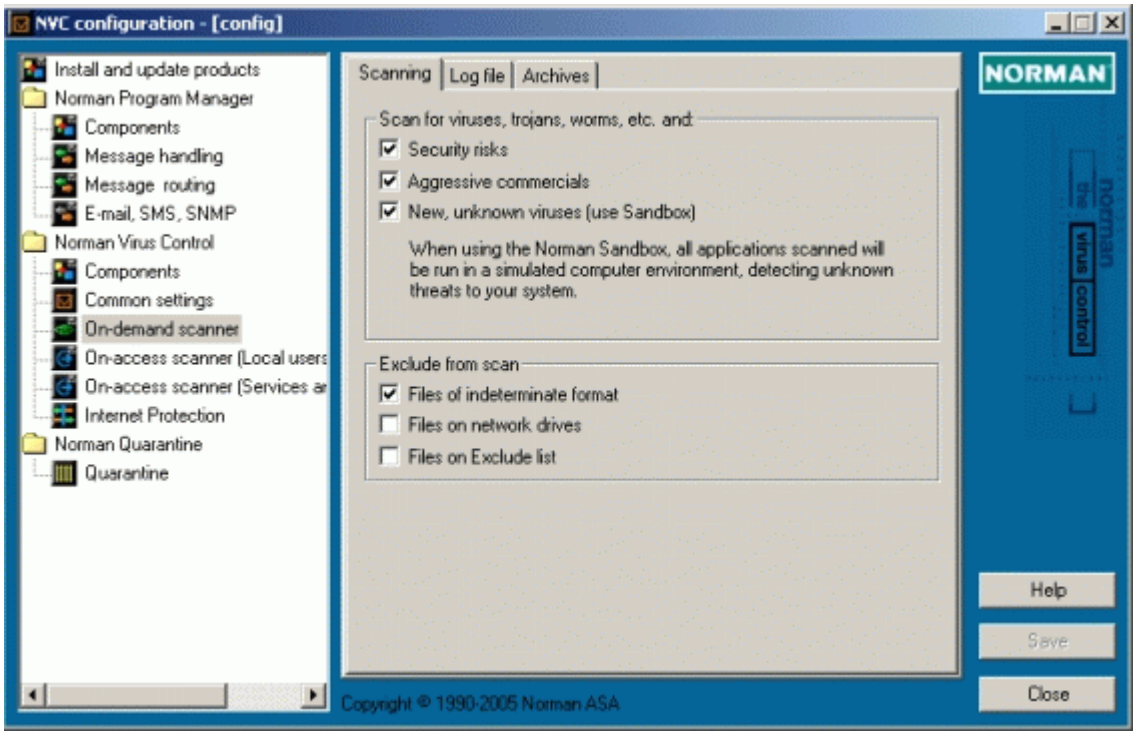
⇨ ‘Shortcut to NVC modules and scanning’ on page 10.

The Right-click scanner will use the settings you specify in the On-demand scanner’s **Scanning** tab, where you can select if the On-demand scanner should use default values or if you want to change them. You can also activate Norman’s Sandbox function from the **Scanning** tab.

⇨ ‘What is a sandbox?’ on page 31

When you run any type of on-demand scan, for example a right-click scan or one of the scans available from the Norman menu, the scanner will use the configuration options that you specify in the three tabs in this dialog:

Copyright © 1990-2005 Norman



When running a right-click scan, you get some additional options, like scanning boot sectors and memory.

The On-access scanner

On-access scanning involves constant monitoring of the file system. Whenever a file is accessed in a read/write operation or a program is executed, the On-access scanner is notified and scans the file on the fly. The On-access module has two tabs:

Scanning, which is divided into three different sections where you can select *scanning strategy*, *files to exclude*, and *how to handle files that cannot be scanned*.

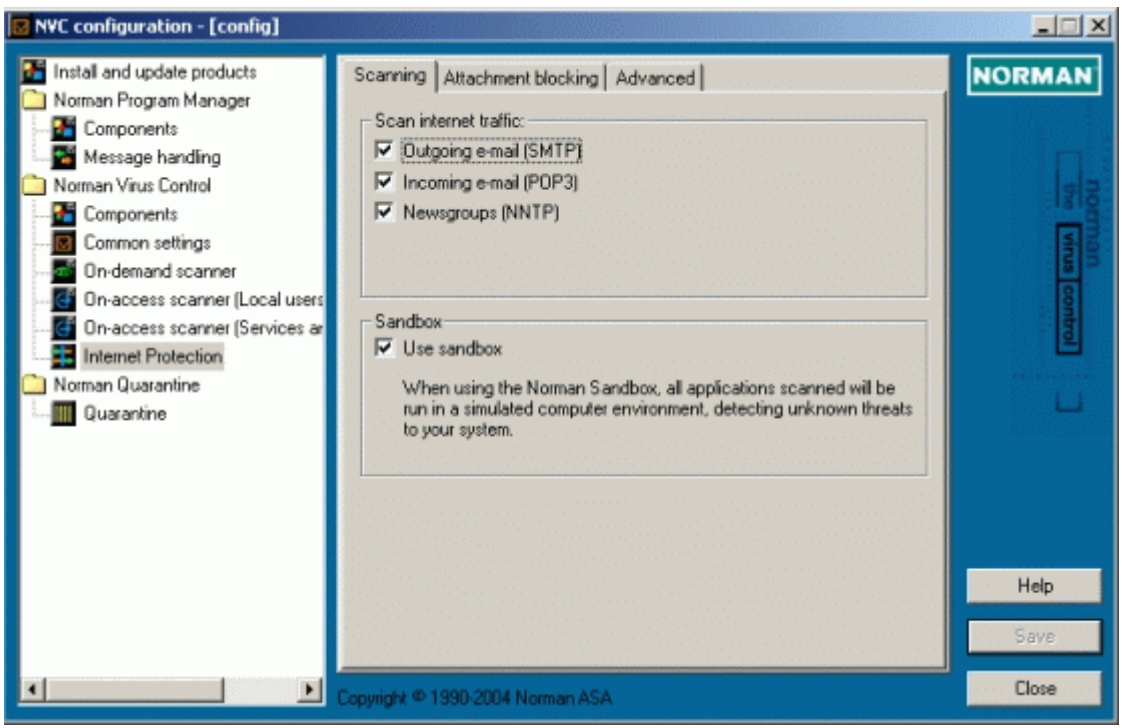
Cleaning, where you determine how infected files should be handled. You can deny access to the file, remove the virus, or prompt for user action.

Copyright © 1990-2005 Norman

On-access scanning on Windows NT/2000/XP includes an additional, configurable module described in the *Reference Guide.*

NVC also runs on Windows Terminal Servers, as described in the *Reference Guide*.

Norman Internet Protection



Note: The current version of Norman Internet Protection is for the Windows platform only, and will *not* work with OS/2.

Norman Internet Protection (NIP) is a filter that protects against viruses that spread through

- Internet mail, and
- news readers.

Copyright © 1990-2005 Norman

The majority of viruses reported today use mechanisms that enable them to spread through e-mail. Statistically, one of 30 e-mails sent during major virus epidemics contains some sort of malicious software. The need for protection against such virus attacks is imperative.

NIP is a NVC 5 module designed to intercept incoming and outgoing mail and news—stripping or blocking all infected attachments for undesired content.

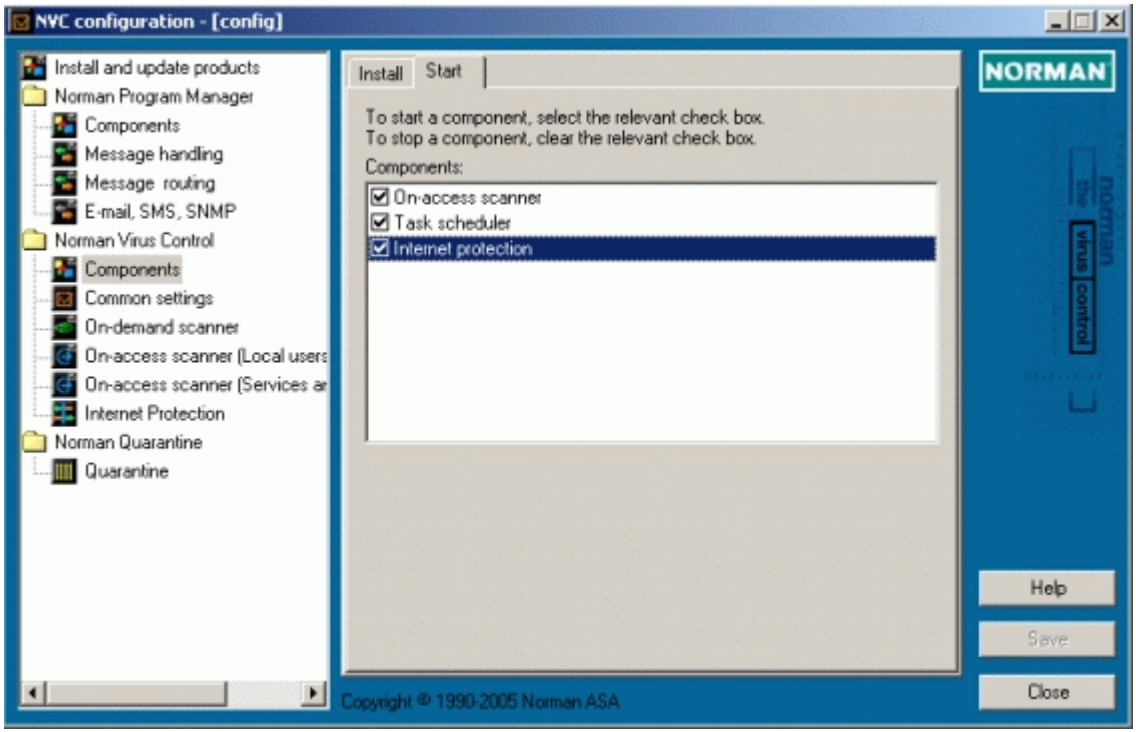
NIP is both capable of scanning e-mails for known viruses and block file attachments, depending on content and file extensions. NIP monitors the most prevalent messaging protocols and supports most popular e-mail clients. As an integrated component in NVC 5 it represents yet another barrier against the increasing threat from e-mail viruses.

Enable NIP

To install this module, go to the **Install** tab in **Components** in the **Norman Virus Control** folder. Select ***Internet protection*** at the bottom of the list and click **Save**.

After a few seconds, ***Internet protection*** appears as a separate entry under the **Start** tab. Again, select it and click **Save**.

Copyright © 1990-2005 Norman



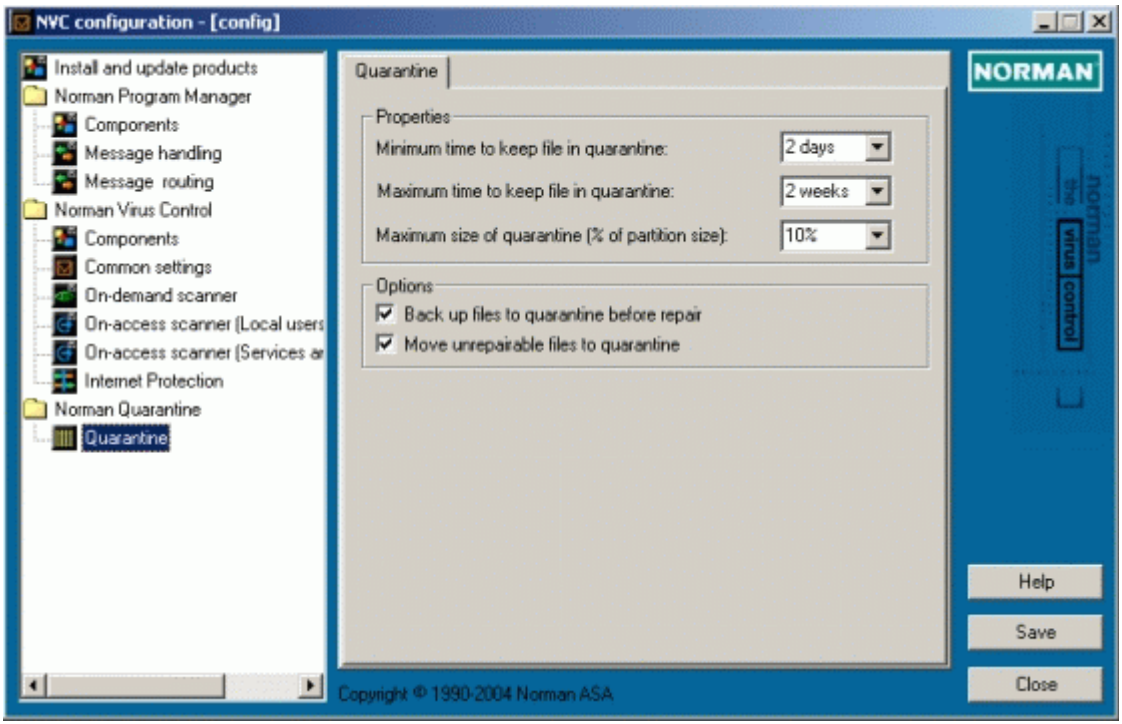
You will have to exit and restart the Configuration Editor to be able to configure NIP's options.

To stop NIP, clear the check box and click **Save**.

Copyright © 1990-2005 Norman

Norman Quarantine

Quarantine

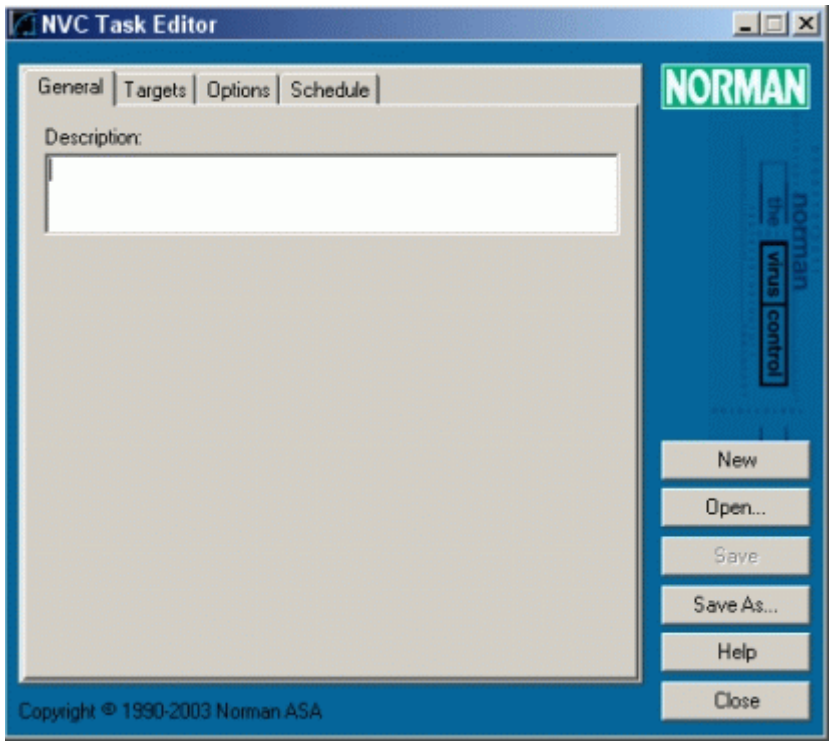


From this tab you decide how to handle files that NVC has identified as infected or in other ways suspicious. If you don't clean or delete such files, we recommended that you isolate them to a designated area, a quarantine.

As more Norman products are added to your existing installation, they will share this quarantine function and use the same options as specified here. Thus you can maintain a consistent quarantine strategy.

Copyright © 1990-2005 Norman

The task editor



You can create a task file for scans that you wish to perform on a regular basis, or special scans that you intend to run in certain situations. For example, if you download files from the Internet to designated areas, you can create a task file that scans these areas only and run the task manually after downloads. In addition, you can schedule the task to run at a preselected time.

Administrators can create task files and distribute them to all workstations in the network to ensure consistent checking of areas that require special attention.

The default location for storing task files is `...\nvc\tasks`. You can view, edit, run, and delete your task files from NVC **Utilities** (see page 28).

Copyright © 1990-2005 Norman

About the scheduler

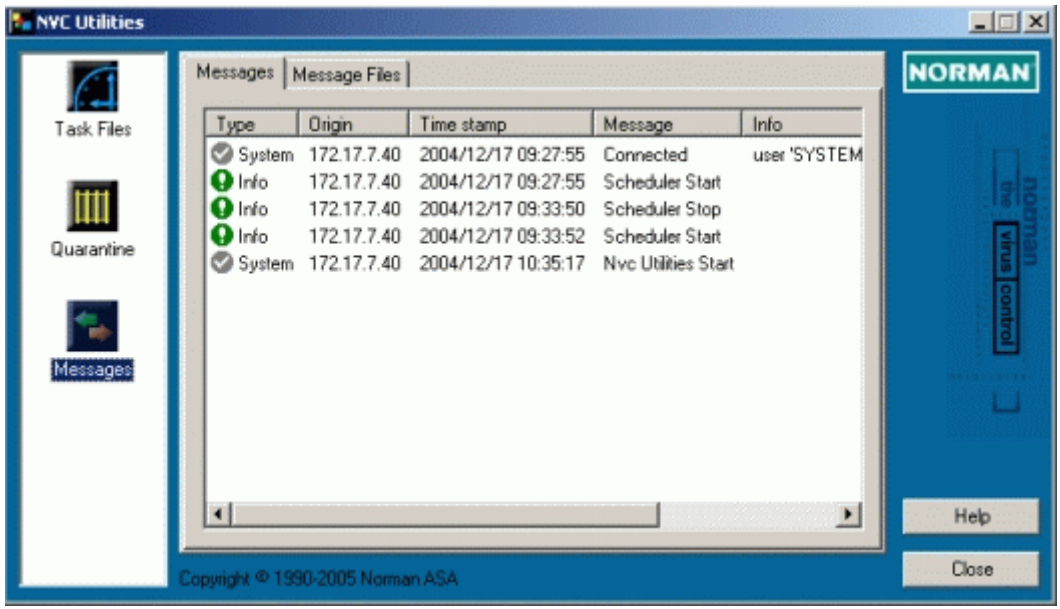
The scheduler's primary objective is to run task files at a specified time. A task file can be scheduled to run daily, weekly, monthly, or just once. You must enter start date and time, and the default values are the current date and time.

For companies with offices in different time zones, the Universal Time Coordinates (UTC) feature permits a task to be run concurrently regardless of time zones.

The scheduler will always look in the subdirectory "Tasks" for scheduled jobs, and it is therefore necessary to keep the structure `...\nvc\tasks` in order to perform a scheduled task.

Copyright © 1990-2005 Norman

Utilities



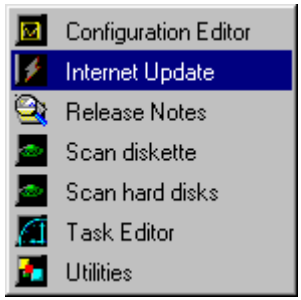
NVC utilities is a tool that presents an overview of certain NVC components on your PC. You can view messages and message- as well as task files. In addition you can change certain elements by selecting some of the entries, for example task files. Other elements provide information only and cannot be edited from the Utilities module.

In this version the utilities group is made up from three modules:

- Task files
- Quarantine
- Messages

Copyright © 1990-2005 Norman

Internet Update



For those who don't update NVC by letting the agent distribute updates in a local network, Norman's Internet Update (IU) is the alternative method. Internet Update is a program that ensures that you are running the current version of NVC for your platform. Any changes to NVC, such as actual program changes, bug-fixes, new scanner engine and updated definition files, are available from Norman's servers. When you run NIU, the program will compare the NVC components installed on your machine with the corresponding version on Norman's server. If date and/or size deviate from the current version, you are offered to download the updates. Theoretically, the entire program can have been changed and therefore subject to download.

NIU appears as a separate item in the Norman group.

To run NIU, you need a TCP/IP (Internet) connection.

Copyright © 1990-2005 Norman

Other functions

NPM - the agent

NPM with its agent deserves a more detailed explanation than the other components—partly because it's fundamental to NVC, partly because it cannot be configured directly, it is invisible and always running. The agent is the main functionality of ***Norman Program Manager (NPM)***, described in the section starting on page 17.

The agent's file name is `Zanda.exe`—short for Zero Administration Network Distribution Agent. The agent—and NPM as such—is the link between those components that need to communicate, and thus essential to NVC.

The agent resides *locally*, i.e. on the workstation. When instructed by the workstation, the agent will fetch files from the server. For example, if the configuration file specifies that the workstation should look for updates at the server every day at noon, it is the agent that *picks up* the files. In addition, the agent will *send* messages from the workstation to the server.

The agent is always running.

These are some of the tasks that the agent takes care of:

- Handle NVC updates.
- Manage all network traffic, like virus alerts, and all other message handling.
- Ensure that the configuration is in accordance with the administrator's requirement for the individual workstation.
- Fetch software updates, new configuration and task files.
- Clean up the quarantine area.
- Features its own scheduler.

Copyright © 1990-2005 Norman

The Command line scanner

In addition to the GUI based On-demand and On-access scanners, NVC offers a command line version of the scanner.

NVC's command line scanner has the same basic functionality as the menu-driven scanners.

The command line scanner is not dependent on any other modules. It can be run from batch files.

From the DOS prompt, go to the folder where the command line scanner is located and type:

```
nvcc /?
```

for a list of available commands. The default location is `...\nvc\bin`.

Please refer to the *Reference Guide* for a complete list of command line option, how to run task files from the command line, and other available features.

What is a sandbox?

Sandbox is the term that best describes the technique that is used to check if a file is infected by an unknown virus. The name is not randomly picked, because the method allows untrusted, possible viral code to play around on the computer – not in the real computer, but in a simulated and restricted area within the computer. The sandbox is equipped with everything a virus expects to find in a real computer. This is a playground where it is safe to let a virus replicate, but where every step is carefully monitored and logged. The virus is exposing itself in the sandbox, and because its actions have been recorded, the cure for this new perpetrator can be generated automatically.

Today, a new e-mail worm can infect ten thousands of workstations in a matter of seconds. Norman's sandbox functionality can prove to be a valuable tool for trapping new destructive code.

Copyright © 1990-2005 Norman

Copyright © 1990-2005 Norman

Index

—A—

administrator's rights 13

—C—

command line scanner 31
Common settings
    Exclude list 19
Component
    Norman Internet Update (NIU) 29
    Task editor 26
    Utilities 28
Conventions iv
ctions v

—D—

deny access 21

—E—

e-mail 18
exclude list 19

—I—

Install and update product 16
    Install 16
    Internet 16
    LAN/WAN 16
install components 16
Internet
    TCP/IP 29
Internet mail 22
Internet update
    IU 29
IU 29

—L—

Linux iv

—M—

malware v
message console 18
Messages
    log file 18
Module
    Install and update product 16
    Message handling 18
    On-access 21

—N—

news readers 22
Norman Program Manager (NPM) 17, 30
NVC manuals v
NVC updates 30
nvc32.exe 31

—O—

On-access scanner
    Cleaning 21
    deny access 21
    exclude files 21
    handle files that cannot be scanned 21
    Scanning 21
    scanning strategy 21
on-access scanner 21
On-demand scanner
    Scanning 20
OS/2 iv

—Q—

quarantine 25

—R—

remove components 16
Requirements, system iv

Copyright © 1990-2005 Norman

rights 13

—S—

Sandbox 20, 31
schedule a task 26
SMS messages 18
SNMP traps 18
System requirements iv
system tray 10

—T—

task file 26
TCP/IP 29
Technical support vi
trojan v

—U—

Universal Time Coordinates 27
Utilities
    Messages 28
    Quarantine 28
    Task files 28

—V—

virus v

—W—

Windows Terminal Servers 22
worm v

—Z—

Zanda 30

Copyright © 1990-2005 Norman